In the claims:

1. (previously presented) A method for publishing a PIN for use in establishing a pairing between a claimant device and a printing device, comprising:

the printing device detecting a local PIN request made by activation of a user interface control element provided by the printing device;

the printing device generating the PIN in response to the local PIN request and without communicating with the claimant device;

the printing device printing the PIN;

receiving a connection request from the claimant device, the connection request including PIN data assembled from the PIN; and

generating a link key using the PIN data, the link key used for device pairing between the claimant device and the printing device.

2. (original) The method of Claim 1, identifying a local request to print a test page as the local PIN request and wherein printing the PIN comprises printing a test page that includes the PIN.

3.-9. (cancelled)

4. (cancelled)

5. (cancelled)

6. (cancelled)

7. (cancelled)

8. (cancelled)

9. (cancelled)

10. (previously presented) The method of Claim 1, further comprising determining the validity of the PIN data prior to generating the link key.

11. (original) The method of Claim 10, wherein determining includes determining if the PIN data corresponds to the PIN, determining if the generated PIN has expired, and rejecting the connection request if the PIN data does not correspond to the PIN or if the PIN has expired.

12. (previously presented) The method of Claim 1, further comprising rejecting the connection request if the connection request is for a function not associated with the PIN data.

13. (previously presented) A method for establishing a pairing between a claimant device and a verifying device, comprising:

detecting a local PIN request made by activation of a user interface control element provided by the verifying device;

generating a PIN in response to the local PIN request and without communicating with the claimant device;

instructing the verifying device to print the PIN;

receiving from the claimant device a connection request for the verifying device, the connection request including PIN data;

determining whether a link key exists for the verifying device;

if a link key exists:

rejecting the connection request if the verifying device is not multi-claimant enabled;

rejecting the connection request if the verifying device is multi-claimant enabled with restricted access and the claimant device is not approved;

otherwise, upon a determination that the PIN data is valid, generating a link key from the PIN data to establish a pairing between the claimant device and the verifying device.

14. (cancelled)

15. (previously presented) The method of Claim 13, wherein the PIN and the PIN data are of the same format and wherein determining the validity of the PIN data includes determining if the PIN data matches the generated PIN.

16. (previously presented) The method of Claim 13, wherein determining the validity of the PIN data comprises:

acquiring a unique identifier for the claimant device;

constructing verifying PIN data using the unique identifier and the generated PIN;

determining if the PIN data matches the verifying PIN data.

17. (previously presented) A method for establishing a pairing between a claimant device and a printing device, comprising:

detecting a local request to print a test page made by activation of a user interface control element provided by the printing device;

generating a PIN in response to the local request to print the test page and without communicating with the claimant device;

instructing the printing device to print a test page that includes the PIN;

receiving from the claimant device a connection request, the connection request including PIN data;

determining whether a valid link key exists exist for the printing device;

if a valid link key exists:

rejecting the connection request if the printing device is not multi-claimant enabled;

rejecting the connection request if the printing device is multi-claimant enabled with restricted access and the claimant device is not approved;

otherwise, upon a determination that the PIN data is valid, generating a link key from the PIN data to establish a pairing between the claimant device and the printing device.

18. (currently amended) A non-transitory computer readable medium having instructions for:

detecting a local PIN request made by activation of a user interface control element provided by a printing device;

generating a PIN in response to a local PIN request and without communicating with the claimant device;

printing the PIN;

receiving a connection request from the claimant device, the connection request including PIN data assembled from the PIN; and

generating a link key using the PIN data to establish a device pairing between the printing device and the claimant device.

19. (cancelled)

20. (cancelled)

21. (previously presented) The medium of Claim 18, wherein the local PIN request is a local request to print a test page, and wherein the instructions for printing include instructions for printing a test page that includes the PIN.

22. (cancelled)

23. (original) The medium of Claim 18, having further instructions for determining the validity of the PIN data prior to generating the link key.

24. (original) The medium of Claim 23, wherein the instructions for determining include instructions for determining if the PIN data corresponds to the PIN, determining if the generated PIN has expired, and rejecting the connection request if the PIN data does not correspond to the PIN or if the PIN has expired.

25. (original) The medium of Claim 18, having further instructions for rejecting the connection request if the connection request is for a function not associated with the PIN data.

26. (currently amended) A non-transitory computer readable medium having instructions for:

detecting a local PIN request made by activation of a user interface control element provided by a verifying device;

generating a PIN in response to a local PIN request and without communicating with the claimant device;

instructing the verifying device to print the PIN;

receiving from a claimant device a connection request, the connection request including PIN data;

determining whether a link key exists for a verifying device;

if a link key exists:

rejecting the connection request if the verifying device is not multi-claimant enabled;

rejecting the connection request if the verifying device is multi-claimant enabled with restricted access and the claimant device is not approved;

otherwise, upon a determination that the PIN data is valid, generating a link key from the PIN data to establish a pairing between the claimant device and the verifying device.

27. (cancelled)

28. (previously presented) The medium of Claim 26, wherein the PIN and the PIN data are of the same format and wherein the instructions for determining the validity of the PIN data include instructions for determining if the PIN data matches the generated PIN.

29. (previously presented) The medium of Claim 26, wherein the instructions for determining the validity of the PIN data include:

acquiring a unique identifier for the claimant device;

constructing verifying PIN data using the unique identifier and the generated PIN;

determining if the PIN data matches the verifying PIN data.

30. (currently amended) A non-transitory computer readable medium having instructions for:

detecting a local request to print a test page made by activation of a user interface control element provided by a printing device;

generating a PIN in response to local request to print a test page and without communicating with the claimant device;

instructing the printing device to print a test page that includes the PIN;

receiving from a claimant device a connection request, the connection request including PIN data;

determining whether a valid link key exists for the printing device;

if a valid link key exists:

rejecting the connection request if the printing device is not multi-claimant enabled;

rejecting the connection request if the printing device is multi-claimant enabled with restricted access, and the claimant device is not approved;

otherwise, upon a determination that the PIN data is valid, generating a link key from the PIN data to establish a pairing between the claimant device and the printing device.

31. (currently amended) A system for publishing a PIN for use in establishing a pairing between a claimant device and a printing device, comprising:

hardware;

a pin module implemented at least by the hardware and operable to receive a local PIN request made by activating a user interface control element provided by a verifying device, the pin module being operable to generate the PIN in response to the local PIN request and without communicating with the claimant device;

a publishing module implemented at least by the hardware and operable to direct a print engine for the printing device to print the PIN;

a connection module implemented at least by the hardware and operable to receive a connection request from the claimant device, the connection request including PIN data assembled from the PIN; and

a key module implemented at least by the hardware and operable to generate a link key using the PIN data, the link key used for paring the claimant device with the verifying device.

32. (original) The system of Claim 31, wherein the local PIN request is a local request to print a test page, and wherein the publishing module is operable to identify the request, to direct the PIN module to generate the PIN, and to direct the print engine to print a test page that includes the PIN.

33. (cancelled)

34. (cancelled)

35. (cancelled)

36. (cancelled)

37. (cancelled)

38. (cancelled)

39. (cancelled)

40. (previously presented) The system of Claim 31, further comprising an authentication module operable to validate the PIN data and to instruct the key module to generate a link key upon a determination that the PIN data is valid.

41. (original) The system of Claim 40, wherein the authentication module is operable to determine if the PIN data corresponds to the PIN, to determine if the generated PIN has expired, and to reject the connection request if the PIN data does not correspond to the PIN or if the PIN has expired.

42. (previously presented) The system of Claim 31, further comprising an authentication module operable to reject the connection request if the connection request is for a function not associated with the PIN data.

43. (currently amended) A system for establishing a pairing between a claimant device and a verifying device, comprising:

hardware;

a PIN module implemented at least by the hardware and operable to receive a local PIN request made by activating a user interface control element provided by a verifying device, the pin module being operable to generate a PIN in response to the local PIN request and without communicating with a claimant device;

a publishing module implemented at least by the hardware and operable to instructing the verifying device to print the PIN;

a connection module implemented at least by the hardware and operable to receive from the claimant device a connection request, the connection request including PIN data;

an authentication module implemented at least by the hardware and operable:

to determine whether a valid link key exists for the verifying device;

to reject the connection request if the verifying device is not multi-claimant enabled and a valid link key exists;

to reject the connection request if the verifying device is multi-claimant enabled with restricted access and the claimant device is not approved;

to determine the validity of the PIN data and reject the connection request upon a determination that the PIN data is not valid; and

a key module operable to generate a link key from the PIN data to establish a pairing between the claimant device and the verifying device.

44. (cancelled)

45. (previously presented) The system of Claim 43, wherein the PIN and the PIN data are of the same format and wherein the authentication module is operable to determine the validity of the PIN data by determining if the PIN data matches the generated PIN.

46. (previously presented) The system of Claim 43, wherein the authentication module is operable to validate the PIN data by:

acquiring a unique identifier for the claimant device;

constructing verifying PIN data using the unique identifier and the generated PIN;

determining if the PIN data matches the verifying PIN data.

47. (currently amended) A system for establishing a pairing between a claimant device and a printing device, comprising:

hardware;

a PIN module implemented at least by the hardware and operable to receive a local request to print a test page made by activating a user interface control element provided by a printing device, the pin module being operable to generate a PIN in response to the local request to print the test page and without communicating with the claimant device;

a publishing module implemented at least by the hardware and operable to instruct the printing device to print a test page that includes the PIN;

a connection module implemented at least by the hardware and operable to receive from the claimant device a connection request, the connection request including PIN data;

an authentication module implemented at least by the hardware and operable:

to determine whether a link key exists for the verifying device and if a link key exists;

to reject the connection request if the verifying device is not multi-claimant enabled;

to reject the connection request if the verifying device is multi-claimant enabled with restricted access and the claimant device is not approved;

to determine the validity of the PIN data and reject the connection request if the PIN data is not determined to be valid; and

a key module operable to generate a link key from the PIN data to establish a pairing between the claimant device and the verifying device.

48. (cancelled)

49. (cancelled)